Research Insights

—

Big tech's privacy crisis: Five crucial questions for 2019 and beyond

What every business needs to know now about trust, data security, and the regulatory environment.

IBM **Institute for Business Value**

IBM

By Brian O'Keefe

Talking points

Consumer concern

People are growing uneasy about trusting organizations with their personal information. According to new research, 81 percent of consumers globally said that in the past year they have become more concerned with how companies are using their data. And 75 percent said they had become less likely to trust companies with their personal data.

Rising regulation

New privacy laws are appearing around the world and multiple privacy bills are being discussed or considered in the US Congress. Among consumers, 87 percent polled globally said that in the past year they had come to believe that companies that are custodians of data need to be more regulated. And 93 percent of global executives agreed that governments will enact more legislation on data transparency.

AI raises the stakes

People want assurance that artificial intelligence will be developed responsibly. Globally, 78 percent of consumers said they generally trust companies to be responsible and ethical in developing new technologies such as AI. But 88 percent agreed that technologies such as AI increase the need for clear policies governing how businesses use personal data.

—

It's hard to pinpoint the precise moment that apathy turned to alarm. It might have been March 2018 when it was reported that a British consulting firm called Cambridge Analytica had obtained and parsed the personal data of 87 million Facebook users, and then sold the insights gained.[1] Or it could have been in June when it emerged that a marketing company called Exactis had left the personal data of 230 million Americans on a publicly accessible server.[2] Or in October, when Google revealed that the personal information of 52 million Google+ users had been exposed.[3]

But there is no question that, as 2019 unfolds, data security and privacy have become central themes for all companies—whether in tech or not—and for watchdogs from media to government.

Recent months have seen a rising wave of discomfort and controversy, as consumers have finally begun to grapple with the trade-off at the heart of many of the wondrous services that technology has spawned—that in exchange for using them, you may not always be turning over money, but you are turning over data. Your own personal data. What you search for. What you buy. Even, oftentimes, your physical location at every moment. And that information is being analyzed, packaged, and sold.

Today's fast-shifting technology and regulatory landscape brings uncertainty for big corporations, small companies, governments, and non-profits. The rules of responsible behavior are changing rapidly, especially with the arrival of emerging technologies such as AI.

In fact, according to fresh research by the IBM Institute for Business Value (IBV), 81 percent of surveyed consumers globally say that in the past year they have become more concerned with how companies are using their data. And 89 percent agree that technology companies need to be more transparent about their products (see Figure 1).

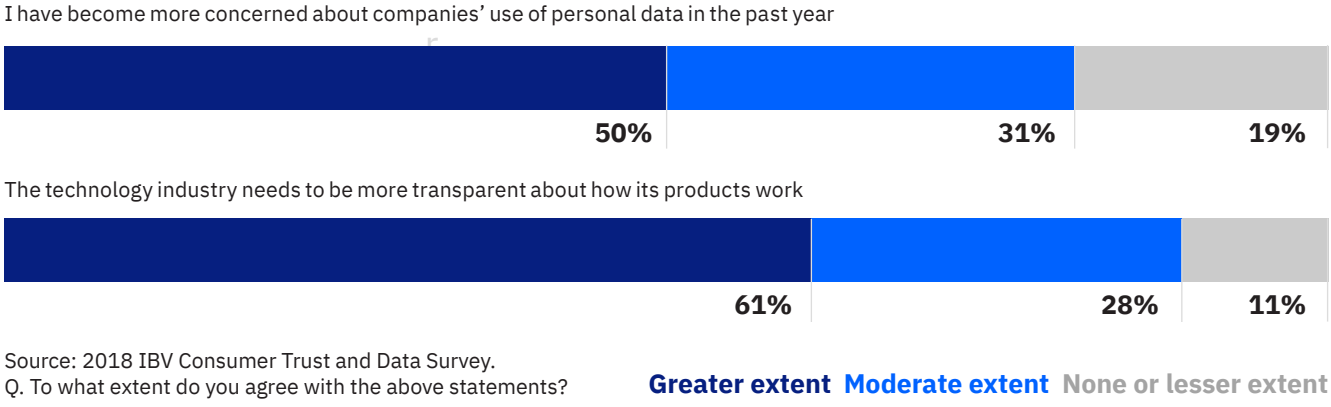
The new level of skepticism about what technology has wrought has taken hold just as society's appetite for privacy risk is being tested in more extreme ways. Tens of millions of consumers have installed voice-enabled digital assistants in their homes—welcoming in listening devices connected to the cloud.[4] Millions more have turned over their DNA information to private companies at the same time that scientists are experimenting with technology like CRISPR to edit genes.[5] Facial recognition technology is growing more sophisticated by the day and its implementation is spreading almost as fast. The rapid development of self-driving cars and digital medical implants is creating new types of systems that could potentially be hacked. And artificial intelligence (AI) is being developed with data-hungry algorithms.

At the same time, a wave of regulatory engagement has sprung up around the globe. In May 2018, the European Union's (EU) General Data Protection Regulation (GDPR), a law designed to give individuals control over their private data, went into effect.[6] In June, the California Consumer Privacy Act of 2018 was passed and signed into law in Silicon Valley's home state—an act that could have a regulatory ripple effect (more on that below).[7] Brazil passed a data protection bill as well last year, and India released a first draft of its own personal data protection law.[8]

What this fast-shifting landscape means is a new level of uncertainty for every type of organization—big corporations, small companies, governments, non-profits. The rules and standards for responsible behavior are changing rapidly, especially with emerging technologies such as AI arriving. "Paradoxically, we are surrounded by information and paralyzed by it," says Amy Webb, the founder of strategy firm the Future Today Institute and the author of a new book called *The Big Nine: How the Tech Titans and Their Thinking Machines Could Warp Humanity*. "We are facing deep uncertainties of a scope and scale that modern humanity hasn't had to grapple with before."

Figure 1

Consumers are increasingly concerned about what personal data companies are using and how they use it



Source: 2018 IBV Consumer Trust and Data Survey.
Q. To what extent do you agree with the above statements?

Consumers, meanwhile, are still struggling to process just how visible their private lives have become in the digital age. For example, according to new IBV research, just 30 percent of consumers reported that they shared personal information with social networks and a mere 32 percent said they share personal data with retailers—suggesting that many people remain in the dark about what and how much companies know about them (see Figure 2). Growing awareness is likely to lead to even more pushback.

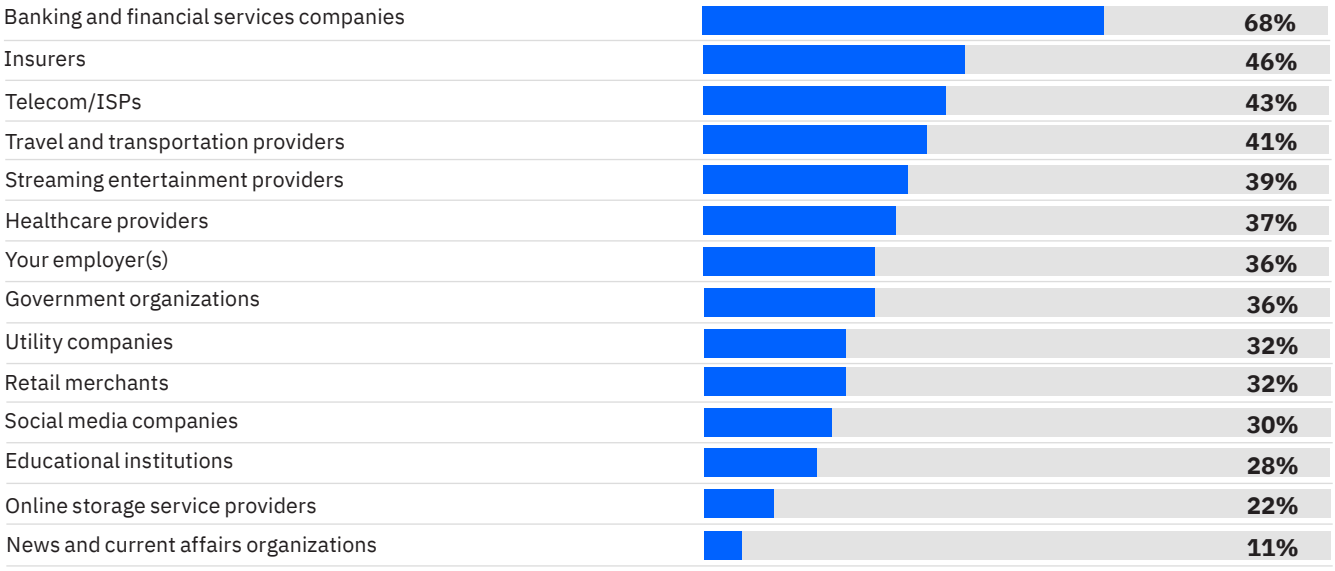
To better understand how attitudes toward privacy and transparency are evolving, the IBV conducted a two-part global study in late 2018. In our AI Ethics Survey, we asked 1,250 executives in 40-plus countries around the world how they expect the debate over privacy and trust to impact their businesses in coming years. Separately, in our Consumer Trust and Data Survey, we polled more than 5,000 consumers in 25 countries to get their opinions on data, transparency, and the technology industry. For context, we interviewed privacy experts and technology industry observers, meshing their insights with our proprietary survey results.

What emerged from this extensive research is a clear message that the conversation about privacy will not be quieting down anytime soon. Below is a framework for understanding how the data challenges will unfold, organized by five essential questions that will shape the debate about technology, trust, and transparency in 2019 and beyond.

—

Figure 2

Consumers report that they are more likely to share personal information with banks and financial services firms than other types of organizations



Source: 2018 IBV Consumer Trust and Data Survey.
Q. With which types of organizations do you share your personal data?

Question No. 1: Will the public maintain its trust in tech?

Despite the public outcry and painful headlines about tech-led assault on privacy in recent months, some business leaders might be tempted to try riding out the storm. They might assess the current brouhaha over privacy as something that can be managed away. And if they choose that strategy, they will have one powerful truth on their side: People want to have faith in the system. They tend to give organizations—even the big tech platforms—the benefit of the doubt.

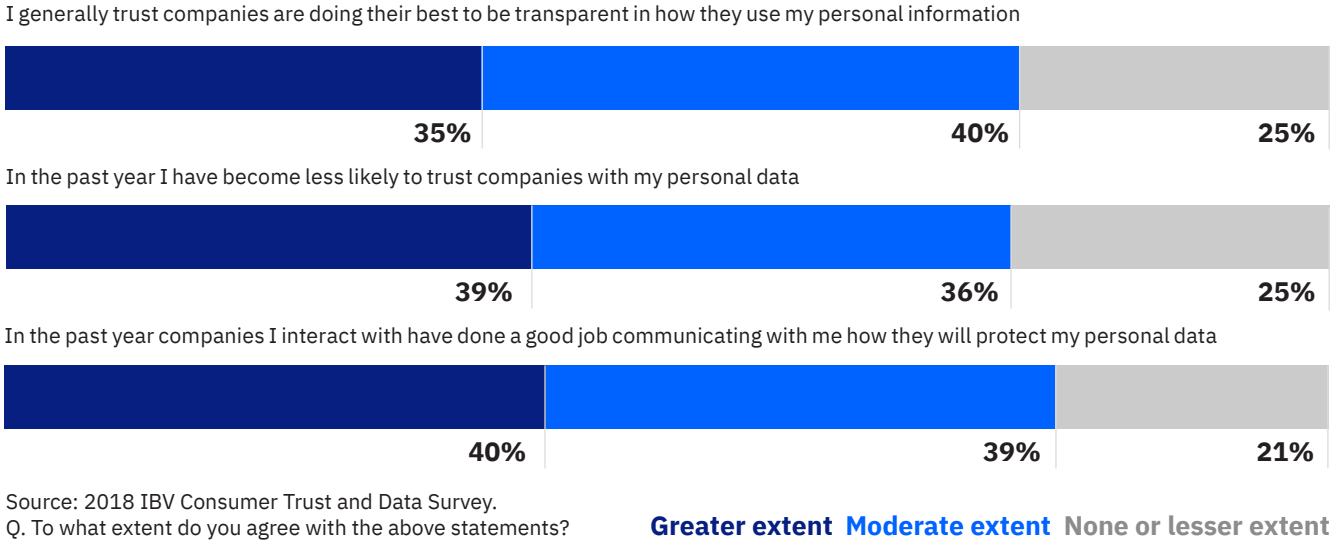
Consider that in the Consumer Trust and Data Survey, 75 percent of global consumers said they agreed that companies generally do their best to be transparent about how they are using personal information (see Figure 3). Our respondents were similarly generous when we asked if they agreed that companies had done a good job in the past year communicating how they would protect their data: 40 percent strongly agreed and another 39 percent moderately assented.

People also tended to be trusting when we asked about the different organizations that handle their data. A mere 8 percent said they trust their employers "to a lesser or no extent" to safeguard their data. Just 9 percent chose the same level of trust to describe their trust in their banks to protect their personal information. Perhaps influenced by headlines about recent data breaches, 15 percent of consumers had lower trust in travel and transportation companies and 22 percent had lower trust in retailers. Social media companies fared worst of all in our study with 32 percent of respondents reporting low trust in them.

But it would be a mistake for executives to hunker down and assume that a business-as-usual strategy will see them through. There is mounting evidence to suggest that the natural trust consumers have in institutions is in danger of eroding. In our global survey, 75 percent of consumers said that in the past year they had become less likely to trust companies with their personal data (see Figure 3).

Figure 3

A majority of consumers agree that companies are trying to be transparent, but they are still growing more concerned about the use of their data



Source: 2018 IBV Consumer Trust and Data Survey.
Q. To what extent do you agree with the above statements?

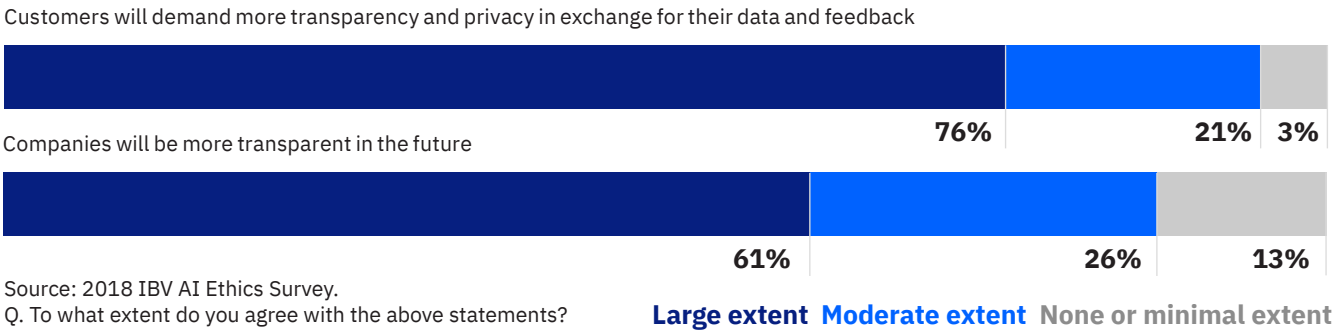
"Over the long-term, companies are going to have to develop more fully fleshed out data policies, even when they're not required to by law."

Lucie Greene, Worldwide Director of the Innovation Group
Wunderman Thompson

—

Figure 4

A vast majority of global executives acknowledge that companies will need to become more transparent, and virtually all agree that customers will demand that transparency



Source: 2018 IBV AI Ethics Survey.
Q. To what extent do you agree with the above statements?

That reality appears not to be lost on executives. In our global survey, 97 percent of respondents agreed when asked if they expect that their customers will demand more transparency and privacy in exchange for their data in the future. And 87 percent agreed that companies will need to be more transparent with customers about their use of data in the future (see Figure 4).

The pressure on all organizations to respond is likely to increase, especially considering that there is a surprisingly large group of consumers globally who don't seem fully clued-in to how vulnerable their data is. Three out of 10 people we polled said they were unaware of massive data breaches that have occurred around the world (see Figure 5). Every time a new hack or data-handling scandal makes the news, the risk rises that public opinion will turn.

"Collectively, all these incidents raise more awareness among consumers of the downside [of technology], even if they still want to use the products," says Lucie Greene, the worldwide director of the Innovation Group at Wunderman Thompson and the author of *Silicon States: The Power and Politics of Big Tech and What It Means for Our Future*. "Over the long-term, companies are going to have to develop more fully fleshed out data policies, even when they're not required to by law."

—

Figure 5

Despite high awareness of breaches, most consumers take little to no consequential action

Source: 2018 IBV Consumer Trust and Data Survey.
Q. Are you aware of data breaches or misuse/mishandling of consumer data by organizations? Actions taken in response?

The most obvious cautionary tale is, of course, Facebook. The social network's *annus horribilis* included the Cambridge Analytica scandal, founder and CEO Mark Zuckerberg's being summoned before Congress in a televised hearing, the news that the data of 29 million Facebook users had been hacked, growing evidence that the platform had been exploited by Russian trolls intending to interfere in US elections, and software snafus such as one that exposed photos of 6.8 million users.[9] Facebook suffered very real consequences at least in part as a result of the mounting scandals.

To keep their customers' trust, companies need to think differently about how they communicate with users.

From its high in July to the end of 2018, Facebook's market value fell by some USD 250 billion.[10] In late December, Pew Research reported that 44 percent of Facebook users it had polled between ages 18-29 had deleted the app from their phones in the past year.[11] And the same month, the Federal Trade Commission said it would examine how Facebook guards the private data of its users.[12]

It's one thing to learn that your data might have been hacked. But it's another to perceive that you are under surveillance. A lot of smartphone users are feeling the latter thanks to a *New York Times* investigation, published in December, of the fast-growing location-tracking industry, which generated an estimated USD 21 billion in targeted advertising in 2018.[13] The *Times* examination found that dozens of companies were able to track and market the precise location of people using apps for weather and other local news functions thanks to the GPS technology on their phones.[14]

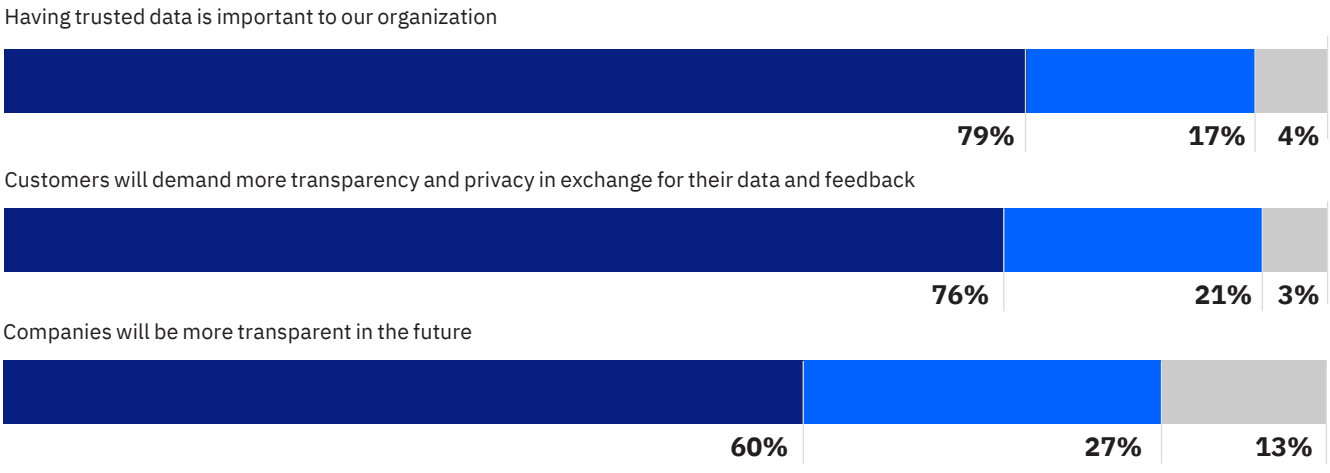
Business leaders can expect to see additional repercussions from these types of revelations in the near future. Given the rapid rate at which companies are developing innovative new digital products and businesses, it is a challenge to bring consumers' understanding along at the same pace—even when organizations are trying their best to be transparent.

Here's some good news: Based on the IBV survey of global executives, leaders of large organizations are well aware of the rising concern and demands for accountability by consumers. According to our research, 97 percent of executives agreed—and 76 percent of them strongly agreed—that over the next three years customers will demand more transparency and privacy in exchange for their data and feedback (see Figure 6). In addition, 96 percent agreed that having trusted data will be important to their organizations. And 87 percent concurred with the idea that companies will be more transparent in the future. To keep their customers' trust, companies need to think differently about how they communicate with users.

—

Figure 6

Executives worldwide agree on the need for trusted data and the need for transparency in the future



Source: 2018 IBV AI Ethics Survey.
Q. To what extent do you agree about the state of AI ethics in the next 3 years?

Question No. 2: Will the US pass a federal digital privacy law?

Guarding personal privacy on tech devices isn't easy. Given all the websites and apps that we use, and how much time it takes to master and manage privacy settings for each one—and to keep up with all the constant updates and changes—most people capitulate. "It's the privacy paradox," says Bob Gellman, a Washington D.C. privacy consultant and former longtime Congressional staffer. "People say they care. But for most people, most of the time, convenience trumps privacy."

That's where regulators—according to more and more consumers—need to step in. The numbers are overwhelmingly clear: In our consumer survey, 87 percent of the people we polled globally said that in the past year they had come to believe that companies that are custodians of data and personal information need to be more regulated (see Figure 7). That desire for more regulation is matched by a belief among executives that increased oversight is coming: 93 percent of executives surveyed agreed that governments will enact increased legislation related to data transparency in coming years.

In fact, the move towards increased regulation on privacy took a couple of big steps forward in 2018—one development that was expected, and a second that surprised many in the tech industry and could have far-reaching consequences in the US. The legal milestone that everyone saw coming was GDPR, the EU law that went into effect in May 2018.[15] Intended to give European citizens more privacy protection and control over their personal information, it effectively established a new baseline for global privacy because all large companies operating in Europe were forced to comply with the EU's standards, or face potential penalties.

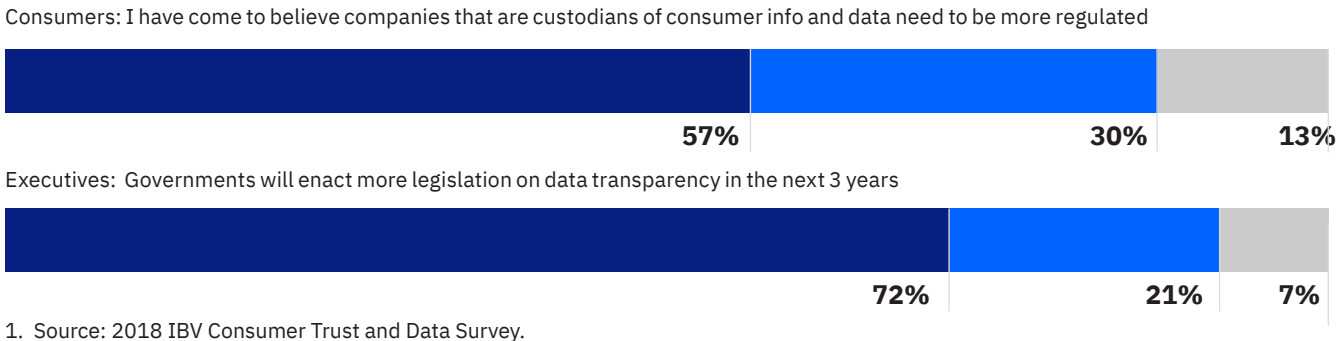
The US tech industry had just begun to live with GDPR when, in June, the California Consumer Privacy Act was passed—a landmark piece of legislation scheduled to go into effect on Jan. 1, 2020.[16] The law was written and passed quickly to preempt a proposed ballot initiative with similar provisions that was facing strong opposition from the technology industry.[17] It has been criticized by some legal experts for being sloppily-constructed, and others for being mis-calibrated and therefore onerous to small businesses.[18] Some privacy advocates bemoan that the legislation leaves out essential protections.[19] Many in Silicon Valley see it as costly and troublesome—a glitch that must be fixed.[20]

But there is no disagreement that the law is groundbreaking: It gives residents of California a range of new rights, including the ability to request that their personal information be deleted and not be sold, and to request an accounting of what data is being compiled about them.[21] In practice, the privacy act could have a huge impact on the business of companies that sell targeted advertising, those that collect and sell data to third parties, and any company that advertises on digital platforms. Enforcement is to be overseen by the California attorney general (AG)—giving the state AG formidable power over any business that has a digital footprint in California.[22]

—

Figure 7

In the past year, consumers say they have come to believe that data custodians need to be more regulated—and executives are expecting increased regulation



1. Source: 2018 IBV Consumer Trust and Data Survey.
Q. To what extent do you agree with the statement?

2. Source: 2018 IBV AI Ethics Survey.
Q. To what extent do you agree with the statement?

> "It's very difficult to write a law for an entire section of the economy even if everyone agrees on the goals—and they don't."
>
> **Peter Swire**, Senior counsel, Alston & Bird

Given that California would be the world's fifth biggest economy if it stood alone from the US, that's a lot of influence.[23] While there is a chance the legislation could be amended before it takes effect, most experts don't expect significant changes.[24]

Yet this is only the beginning. The next big regulatory battle will be in Washington, D.C., where efforts are underway to pass a US federal privacy law.[25] While Silicon Valley tends to be reflexively anti-regulation, it now finds itself leaning into the D.C. regulatory process out of necessity. In fact, some are even hopeful that a federal law might preempt the California legislation, as well as other state laws that could be passed in coming months. "The big tech companies don't want more law, they want one law," says Eric Goldman, a law professor and co-director of the High Tech Law Institute at the Santa Clara University School of Law. Adds Goldman: "So much of the discussion is being driven by anger towards Facebook. Regulating angry is not a good solution."

Privacy regulation has been tried at the federal level and failed before, points out Dipayan Ghosh, formerly privacy and public policy advisor for Facebook and currently the Pozen fellow at the Shorenstein Center at Harvard's Kennedy School where he co-directs the new "platform accountability" initiative. As a technology and economic policy advisor in the White House during the Obama administration, Ghosh worked on the Consumer Privacy Bill of Rights Act that was put forward in 2015 but never passed. "What is different now, though, is that the industry, and especially the companies that will be most affected by privacy regulation, realizes that if it doesn't support legislation, tech companies will be juicy targets for regulators around the world," says Ghosh.

That reality plus the litany of privacy scandals in 2018, combined with the political shift after the midterm elections, means that there is more talk in Washington about a federal privacy bill than there has been in years. In December, for example, US Senator Brian Schatz, a Democrat from Hawaii, introduced a piece of legislation called the Data Care Act, that would require online service providers to ensure consumers a range of rights.[26] And in January, Republican Senator Marco Rubio of Florida floated his own bill, called the American Data Dissemination Act, that would let the Federal Trade Commission make recommendations to Congress about what the rules should be for commercial services.[27]

Despite all that momentum, though, legal experts and Washington insiders say there are still a multitude of obstacles that will make it challenging to get a universal privacy bill passed by Congress and signed into law. "Privacy covers the entire information economy," says Peter Swire, senior counsel with the law firm of Alston & Bird, and a leading privacy and cyber-law scholar and practitioner. "It's very difficult to write a law for an entire section of the economy even if everyone agrees on the goals—and they don't."

Swire and other experts point out that there is already a complex mosaic of privacy regulation in the US: hundreds of state privacy laws, in addition to the many pieces of federal legislation passed over the decades, including the Fair Credit Reporting Act, the Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and even a Video Privacy Protection Act governing video rental outlets. All of these laws apply different standards that would have to be justified.

No one in Washington has answers for how to reconcile a new law with the jumble of existing laws. Not to mention how to address the innumerable questions that will inevitably arise in the crafting of a new piece of legislation. "I don't think anybody has grappled with the actual complexity of privacy law," says Swire. "Congress certainly hasn't grappled with it."

In any federal bill, privacy advocates will drive a long list of demands—meaningful opt-in consent, greater transparency of data use, the so-called right to be forgotten, and stronger security standards, to name a few. Silicon Valley's representatives will likely push back hard on most. "In the tech industry there is so much potential for growth that it's often unclear how new forms of regulation would harm the long-term viability and value of the business model, so they're likely to try to water down everything that comes forward in new privacy bills," says Ghosh.

Finally, there's the political reality: How long will the issue remain at the top of the agenda for Congress? It may take years before a federal bill can pass, especially given all of the partisan battles going on in D.C. Will the already-looming 2020 presidential election delay action further, or provide impetus to act now? What's clear is that privacy issues have broken into broad cultural and political dialogue, and that seems likely only to intensify. Thanks to initiatives like the California law, the mostly unfettered landscape that the tech giants have enjoyed is shifting. And more is on the horizon.

Question No. 3: What's the next move for regulators worldwide?

The United States, sometimes referred to in the past as "the world's policeman," may not end up the ultimate arbiter of tech regulation. Global forces are gathering to fill the void—a situation that encourages some and dismays others.[28]

With the passage of GDPR, the EU sent notice that it was asserting its authority.[29] The primary targets of the law were generally seen as the global technology platforms and social media companies. Yet it's unclear how aggressive the EU will be in applying GDPR. It has certainly rallied action, with more than 95,000 complaints filed to date. But so far there haven't been many large-scale enforcement actions.[30] Last July, the national privacy regulator in Portugal fined a hospital outside Lisbon EUR 400,000 for allowing too many staff members to have access to patients' records.[31] In January, a more high-profile judgement was meted out when France's data protection regulator said it was fining Google EUR 50 million for not properly disclosing to users how their data was being collected and used.[32]

The incidents underscore a hard truth about the brave new world of privacy regulation: Every company and organization must reassess how it operates and what its standards are. Because the bulls-eye may land where we least expect it.

Meanwhile, European regulators are revving up for more action, with the EU and individual countries weighing new permutations for governing behavior in the digital realm. Among the initiatives adopted by the EU institutions is the Platform-to-Business Regulation, designed to bolster the rights of smaller operators reliant on big digital platforms, and end "unfair contractual clauses and trading practices."[33] Another new law, the Directive on Copyright in the Digital Single Market, makes web platforms increasingly liable for copyright material made available online.[34]

There is also a push for increased taxation on global Internet giants—not just from the European Commission (which spent much of 2018 debating the terms of a potential new digital services tax, which would have taxed 3 percent of revenue of digital operators).[35] In fact, several countries, including France, Italy, and Spain, have decided to move forward with their own taxation plans.[36]

As for GDPR, it will only have a greater impact moving forward, asserts Santa Clara University's Goldman, echoing the sentiment of others in the privacy and legal community that more high-profile enforcement is coming in 2019. "The enforcers have been tolerant so far," says Goldman, as companies adjust to the new law. But that patience won't last: "That's their job—to go crack skulls. They'll be cracking skulls soon."

As our consumer survey reveals, the expectation of good behavior by institutions varied widely, and often unpredictably in different countries.

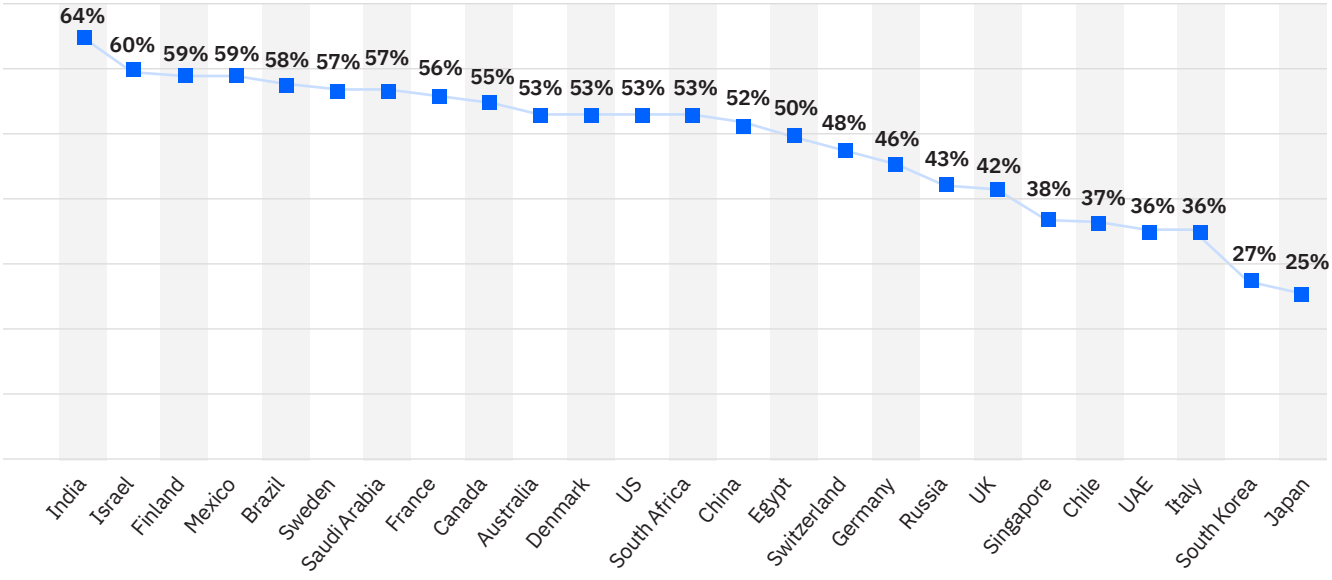
If you expand the purview wider, the privacy landscape gets even more complex. As our consumer survey reveals, the expectation of good behavior by institutions varied widely, and often unpredictably in different countries. When asked if they generally trusted organizations with their personal information, consumers with the highest levels of trust were in India (64 percent) and Israel (60 percent). Levels of trust then gradually declined among countries, with South Korea (27 percent) and Japan (25 percent) reporting the lowest levels (see Figure 8).

On the surface, China would appear to be on the opposite end of the privacy spectrum from Europe. Whereas EU officials talk about data privacy as a constitutional right, the Chinese government has a centralized approach to collecting and analyzing data of its citizens. Since 2014, China has been developing a "social credit" system to rank the trustworthiness of people not just on traditional metrics like loan repayment, but also on the basis of online activity and behavior in their everyday lives.[37] The system, planned to launch in 2020, has engendered much debate. But China also has passed an Internet Security Law, modeled on GDPR, that imposes strict privacy rules on China's internet companies.[38]

The upshot is that digital companies should expect new and shifting privacy standards no matter where they operate. Regulators from Japan to India to Brazil are becoming more assertive.[39] Achieving a global standard for privacy guidelines will be at least as tricky as pushing through a unifying federal law in the US.

Figure 8

Average level of trust in organizations to protect personal information, by country



Source: 2018 IBV Consumer Trust and Data Survey.
Average extent of trust across types of organizations within each country.

Question No. 4: What's the best way to make data privacy and AI compatible?

In December 2018, the European Commission's expert group on AI released a draft version of its ethics guidelines for creating "trustworthy AI," the final version of which will be published in April. Among the fundamental requirements was data governance, including the preservation of privacy. "Artificial intelligence is one of the most transformative forces of our time," reads the report, "and is bound to alter the fabric of society."[40]

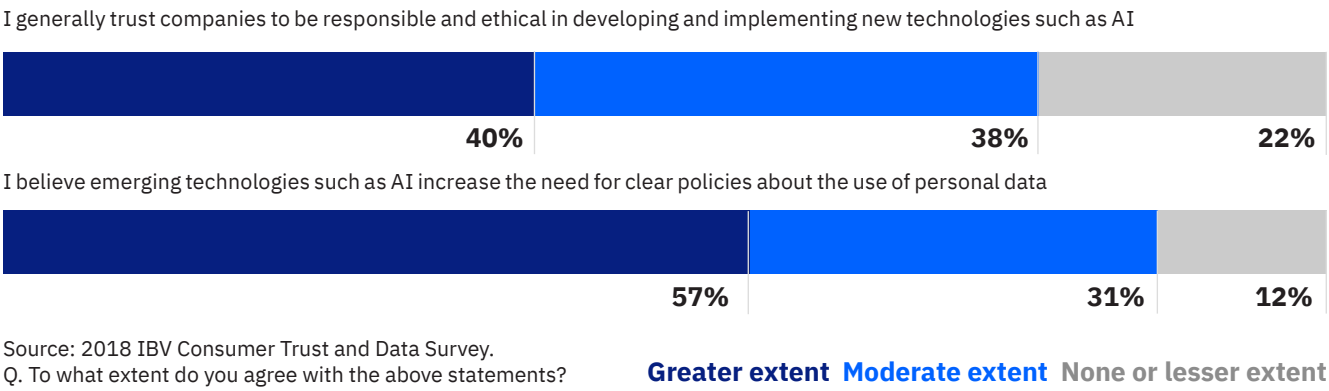
Data is crucial in the development of AI. Gobs of it. Creating sophisticated, effective artificial intelligence requires training the underlying algorithms on massive amounts of information—authentic, real-world data. And that puts privacy on yet another collision course with policy.

Consumers are hungry for reassurance and visibility when it comes to AI. As with tech more broadly, people are inclined to trust organizations: In our survey of global consumers, 78 percent of respondents said they generally trust companies to be responsible and ethical in developing and implementing new technologies such as AI. However, they want greater clarity on how data is being used in the creation of these systems. Asked if they felt that the emergence of technologies like AI increased the need for clear policies about the use of personal data, 88 percent of people agreed—and 57 percent strongly agreed (see Figure 9).

—

Figure 9

A strong majority of consumers trust companies to be responsible in developing new technologies like AI, but they also want to see clear policies articulated



Source: 2018 IBV Consumer Trust and Data Survey.
Q. To what extent do you agree with the above statements?

Safeguarding data is a core competency for getting AI right—and executives that we surveyed made that clear.

Here's one thing we know: AI development will almost certainly speed ahead regardless. The pressure to find competitive advantage will push companies forward in building the technology, with regulation playing catch-up. That raises the importance of getting the right government policies in place now, not later. AI has the potential to make companies run more efficiently and to help us take on societal challenges, such as global health care and climate change. "Business has to make smarter decisions," says Webb, the strategist and author of *The Big Nine*. "Any effort to advance that is in the service of humanity."

Safeguarding data is a core competency for getting AI right—and executives that we surveyed made that clear. We asked leaders in our AI Ethics Survey to rate the relative importance of a range of factors for developing ethical AI, including value alignment, algorithmic accountability, and inclusion. The criterion they ranked No. 1 in importance: "data responsibility."

The vast majority of corporate leaders appear to be expecting societal pressure around AI. In our survey, 92 percent of global executives agreed that their customers will demand more transparency into how the technology that powers AI works. And almost the same portion—91 percent—said that they expect more regulation on AI ethics. More and more companies will be pressed to turn those expectations into action.

Question No. 5: How much privacy risk will consumers tolerate?

The way Bruce Schneier sees it, the trade-off between privacy and functionality is fast becoming a life or death issue. The security guru and Special Advisor to IBM Security points out that computers are controlling everything from self-driving cars to implantable medical devices, and that raises the stakes on keeping systems safe. "Privacy is now a matter of public safety," says Schneier, the author of more than a dozen books, including *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. "It used to be that your data got hacked and you lost some money. Now, you could have your car get hacked and lose your life."

It's an extreme way of framing an essential question: In today's ever-more-digital world, how much risk are people willing to tolerate in the name of new and improving technologies? And then there's the flipside: What are we willing to give up in order to limit unintended consequences? If, for example, security is of paramount importance, then the resources to support security must increase—even if that strains the bottom line.

Based on our survey research, people have mixed feelings about the tech trade-off. On balance, we asked, are the benefits derived from new technology worth sacrificing some privacy? The responses were hardly definitive: 65 percent of respondents agreed with the statement, but only 30 percent strongly agreed. And 35 percent disagreed. In other words, nearly a third of people aren't comfortable with the bargain they're getting from technology.

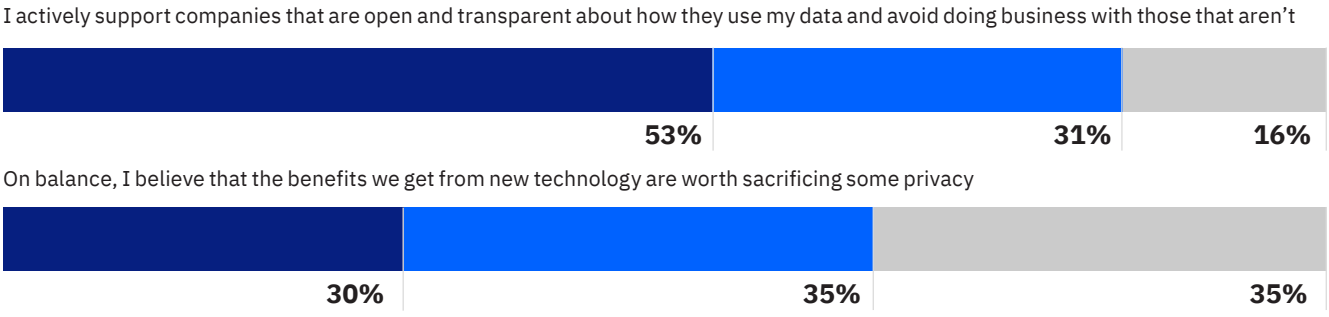
When we asked if they back up their beliefs with actions, the result was a bit clearer: 84 percent of the respondents said that they actively support companies that are transparent about how they use their data and that they avoid doing business with companies that don't (see Figure 10).

It is only going to get harder for consumers to separate their private behavior from the connected world. As Lucie Greene of Wunderman Thompson points out, voice-activated digital assistants or responsive visual recognition technology are changing the way that we react to the Internet, making it more like the air around us. "It's really cool, but I think it removes a layer of mindfulness," says Greene. "The whole human experience is becoming a commodity, something that can be sold and analyzed. The convenience is just too seductive for consumers to reject."

—

Figure 10

Consumers tend to support companies that are more open and transparent about personal data use, despite being mixed about the trade-offs with benefits from new technology



Source: 2018 IBV Consumer Trust and Data Survey.
Q. To what extent do you agree with the above statements?

Greater extent **Moderate extent** None or lesser extent

Companies that make it easier for consumers to take control of and maintain their privacy while engaging in the digital world could gain a competitive advantage going forward.

Younger consumers appear to be less concerned about the trade-off. In the Consumer Trust and Data Survey, we asked respondents who should have responsibility for protecting personal information—organizations that collect and use the data, tech companies that make products for them, government, or the individuals themselves. Consumers of all ages put the most responsibility on the organizations collecting the data and the least on themselves as individuals. But the younger the demographic, the less they pinned culpability on anyone. Just 52 percent of members of Generation Z, for example, say that government should be responsible for protecting personal data versus 64 percent of Millennials and 68 percent of Generation X (see Figure 11).

Any way you cut it, the status quo is not sustainable, argues Jennifer King, director for consumer privacy at the Stanford Law School's Center for Internet and Society.

That's because the current privacy framework puts the bulk of the decisions and responsibility on consumers. "There's this fiction that assumes that you can take control over all of your data," says King. "But you're not given a real choice. It's take the terms or leave them—no negotiation. You cannot expect human beings to manage these things. Even if you did, you're not giving them a manageable way to do it."

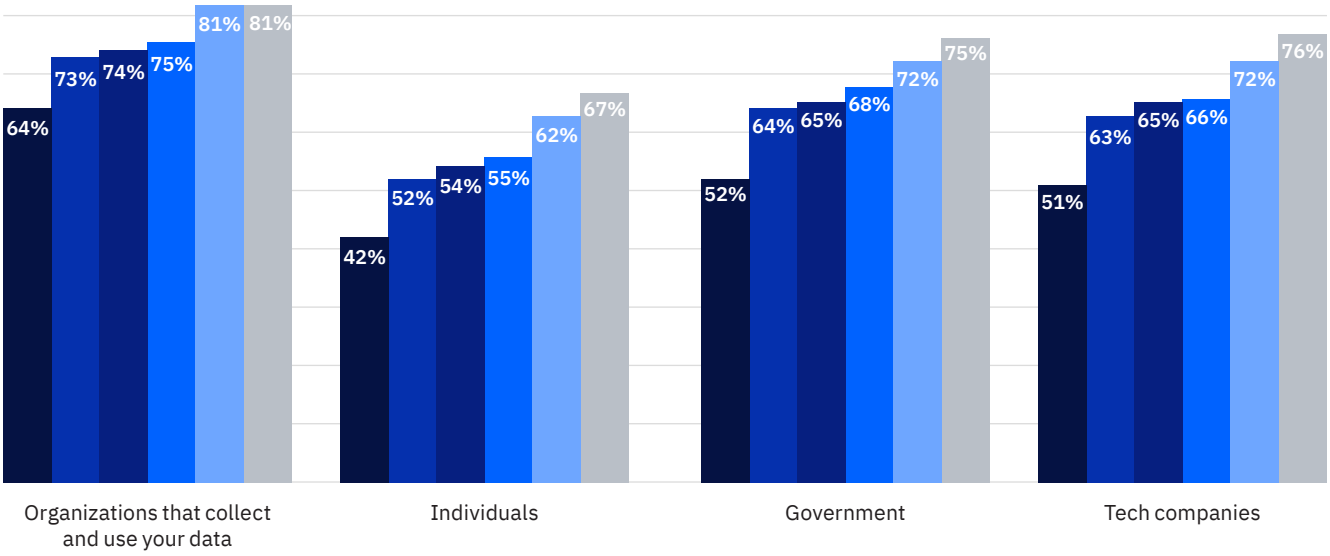
In that sense, privacy is a tremendous opportunity. Companies that make it easier for consumers to take control of and maintain their privacy while engaging in the digital world could gain a competitive advantage going forward. "I'd like to see us turn that corner," says King.

One thing is for sure: Those organizations that get in front of trust and privacy challenges will be better positioned to master them and come out ahead, with governments, regulators, consumers, and business partners.

—

Figure 11

Younger consumers are less concerned about organizations taking responsibility for protection of personal data



Generation (age ranges): **Gen Z** (18-21) **Millennials** (22-37) **All respondents** **Gen X** (38-55) **Boomers** (56-70) **Silent/greatest** (71+)

Source: 2018 IBV Consumer Trust and Data Survey.
Q. Who should have responsibility for protecting personal information?

About the author

Brian O'Keefe
linkedin.com/in/brian-o-keefe-4901615/
Twitter @brianbokeefe
brian.okeefe@ibm.com

Brian O'Keefe is the Editor-in-Chief of the IBM Institute for Business Value, overseeing all editorial strategy and production. Brian came to IBM with two decades of experience as a journalist, most recently serving as the deputy editor at Fortune, where he helped guide all print and digital operations.

Related reports

Wielding a double-edged sword: Preparing cybersecurity now for a quantum world. https://www.ibm.com/thought-leadership/institute-business-value/report/quantumsecurity

The end of the beginning: Unleashing the transformational power of GDPR. https://www.ibm.com/thought-leadership/institute-business-value/report/gdpr

From data deluge to intelligent insights: Adopting cognitive computing to unlock value for marketing and sales. https://www.ibm.com/thought-leadership/institute-business-value/report/cognitivemarketingsales

For more information

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our monthly newsletter, visit: **ibm.com**/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for phone or tablet from your app store.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value (IBV), part of IBM Services, develops fact-based, strategic insights for senior business executives on critical public and private sector issues.

How IBM can help

Get fast, laser-focused incident response with Intelligent Orchestration from IBM Resilient.
ibm.com/security/intelligent-orchestration

About Research Insights

Research insights are fact-based strategic insights for business executives on critical public and private sector issues. They are based on findings from analysis of our own primary research studies. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

Notes and sources

1 Lapowsky, Issie. "Facebook Exposed 87 Million Users to Cambridge Analytica." WIRED.com. April 4, 2018. https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

2 Meyer, David. "A New Data Leak Reportedly Exposed 230 Million Americans' Personal Information." *Fortune*. June 28, 2018. http://fortune.com/2018/06/28/exactis-data-leak-personal-information/

3 Tarantola, Andrew. "Another Google+ data bug exposes info for 52.5 million users." *Engadget*. December 10, 2018. https://www.engadget.com/2018/12/10/google-plus-data-leak-info-52-5-million/

4 Perez, Sarah. "47.3 million U.S. adults have access to a smart speaker, report says." *Tech Crunch*. March 7, 2018. https://techcrunch.com/2018/03/07/47-3-million-u-s-adults-have-access-to-a-smart-speaker-report-says/

5 "Behind at-home DNA testing companies sharing genetic data with third parties." CBS News. August 2, 2018. https://www.cbsnews.com/news/dna-privacy-at-home-tests-23andme-ancestrydna-sell-data-to-third-parties/; Leavenworth, Stuart. "Who is the secretive Google offshoot that has access to Ancestry's DNA database?" McClatchy DC Bureau. June 1, 2018. https://www.mcclatchydc.com/news/nation-world/article211324909.html; Plumer, Brad, Eliza Barclay, Julia Belluz and Umair Irfan. "A simple guide to CRISPR, one of the biggest science stories of the decade." Vox. December 27, 2018. https://www.vox.com/2018/7/23/17594864/crispr-cas9-gene-editing

6 Hern, Alex. "What is GDPR and how will it affect you?" *The Guardian*. May 21, 2018. https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you

7 McCreary, Mark. "The California Consumer Privacy Act: What You Need to Know." *New Jersey Law Journal*. December 1, 2018. https://www.law.com/njlawjournal/2018/12/01/the-california-consumer-privacy-act-what-you-need-to-know/

8 Ramey, Melanie. "Brazil's New General Data Privacy Law Follows GDPR Provisions." *Inside Privacy*. August 20, 2018. https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/; Merwin, Radhika. "All you wanted to know about Personal Data Protection Bill 2018." *The Hindu Business Line*. August 6, 2018. https://www.thehindubusinessline.com/opinion/columns/slate/all-you-wanted-to-know-about/article24617362.ece

9 Sutton, Kelsey. "Facebook's Terrible, Horrible, No Good, Very Bad Year." *Adweek*. https://www.adweek.com/digital/facebooks-terrible-horrible-no-good-very-bad-year/; Wong, Queenie and Laura Hautala. "Facebook says hackers stole personal info on 29 million users." Cnet.com. October 12, 2018. https://www.cnet.com/news/facebook-e-mails-phone-numbers-and-other-personal-information-accessed-during-breach/

10 IBM Institute for Business Value analysis of company stock history. Bloomberg. https://www.bloomberg.com/quote/FB:US. Accessed on February 20, 2019.

11 Rosoff, Matt. "Facebook exodus: Nearly half of young users have deleted the app from their phone in the last year, says study." CNBC. September 5, 2018. https://www.cnbc.com/2018/09/05/facebook-exodus-44-percent-of-americans-age-18-29-have-deleted-app.html

12 Facebook May Have Breached a 2011 Consent Agreement, FTC Says." *Fortune*. March 29, 2018. http://fortune.com/2018/03/29/cambridge-analytica-facebook-scandal/

13 Valentino-DeVries, Jennifer, Natasha Singer, Michael H. Keller and Aaron Krolik. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." *The New York Times*. December 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

14 Ibid.

15 Hern, Alex. "What is GDPR and how will it affect you?" *The Guardian*. May 21, 2018. https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you; Handley, Lucy. "US companies are not exempt from Europe's new data privacy rules — and here's what they need to do about it." CNBC. April 25, 2018. https://www.cnbc.com/2018/04/25/gdpr-data-privacy-rules-in-europe-and-how-they-apply-to-us-companies.html

16 McCreary, Mark. "The California Consumer Privacy Act: What You Need to Know." *New Jersey Law Journal*. December 1, 2018. https://www.law.com/njlawjournal/2018/12/01/the-california-consumer-privacy-act-what-you-need-to-know/

17 Woolfolk, John. "California data privacy bill signed to head off ballot initiative." *Santa Cruz Sentinel*. June 28, 2018. https://www.santacruzsentinel.com/2018/06/28/california-data-privacy-bill-signed-to-head-off-ballot-initiative/

18 Ross, Andrew. "Big tech firms want to "clean-up" the new California Consumer Privacy Act 2018." *Information Age*. August 24, 2018. https://www.information-age.com/big-tech-want-to-clean-up-californias-new-privacy-law-123474381/

19 Schwartz, Adam, Lee Tien and Corynne McSherry. "How to Improve the California Consumer Privacy Act of 2018." Electronic Frontier Foundation website. August 8, 2018. https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018

20 Ross, Andrew. "Big tech firms want to "clean-up" the new California Consumer Privacy Act 2018." *Information Age*. August 24, 2018. https://www.information-age.com/big-tech-want-to-clean-up-californias-new-privacy-law-123474381/

21 McCreary, Mark. "The California Consumer Privacy Act: What You Need to Know." *New Jersey Law Journal*. December 1, 2018. https://www.law.com/njlawjournal/2018/12/01/the-california-consumer-privacy-act-what-you-need-to-know/

22 Heck, Zachary. "Change is in the California Air as Legislature Amends New Privacy Law." Privacy & Data Security Insight. October 22, 2018. https://www.privacyanddatasecurityinsight.com/2018/10/change-is-in-the-california-air-as-legislature-amends-new-privacy-law/

23 Cooper, Jonathan J. "California now world's 5th largest economy, surpassing UK." *USA Today*. May 5, 2018. https://www.usatoday.com/story/news/nation-now/2018/05/05/california-now-worlds-5th-largest-economy-beating-out-uk/583508002/

24 Heck, Zachary. "Change is in the California Air as Legislature Amends New Privacy Law." Privacy & Data Security Insight. October 22, 2018. https://www.privacyanddatasecurityinsight.com/2018/10/change-is-in-the-california-air-as-legislature-amends-new-privacy-law/

25 NG, Alfred. "Senator's data privacy law draft could put CEOs in jail for lying." Cnet.com. November 1, 2018. https://www.cnet.com/news/senator-introduces-privacy-law-draft-that-could-put-ceos-in-jail-for-data-breaches/; Bartz, Diane. "U.S. senator says privacy bill draft could come early next year." Reuters. November 27, 2018. https://www.reuters.com/article/us-usa-ftc-congress/u-s-senator-says-privacy-bill-draft-could-come-early-next-year-idUSKCN1NX041

26 Cameron, Dell. "Democrats Want Internet Companies to Be Liable for Data Loss Like Banks and Hospitals." Gizmodo. December 12, 2018. https://gizmodo.com/democrats-want-internet-companies-to-be-liable-for-data-1831051736; Lecher, Colin. "Democratic senators have introduced a big new data privacy plan." *The Verge*. December 12, 2018. https://www.theverge.com/2018/12/12/18138131/democratic-data-care-act-senate-law

27 American Data Dissemination Act. "S.142 – ADD Act." Current legislation, 116th Congress. Congress.gov. https://www.congress.gov/bill/116th-congress/senate-bill/142?q=%7B%22search%22%3A%5B%22data+collection+and+dissemination+rubio%22%5D%7D&s=1&r=1

28 Geller, Eric. "China, EU seize control of the world's cyber agenda." Politico. July 19, 2018. https://www.politico.eu/article/china-eu-dominate-cyber-agenda-us-on-tech-sidelines/; Fritz, Gernot. "First GDPR fine issued by Austrian data protection regulator." Freshfields Bruckhaus Deringer. October 5, 2018. https://digital.freshfields.com/post/102f39w/first-gdpr-fine-issued-by-austrian-data-protection-regulator

29 EUR-Lex: Access to European Union law. Document 32016R0679. Summary of legislation – "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)." http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679

30 Baxter, Anne Shannon. "How GDPR Enforcement Is Shaping Up In Europe." *Corporate Compliance Insights*. December 13, 2018. https://www.corporatecomplianceinsights.com/how-gdpr-enforcement-is-shaping-up-in-europe/

31 Rasmussen, Kristen. "GDPR Fine Against Portuguese Hospital Puts Health Care Providers on Alert." *Corporate Counsel*. November 9, 2018. https://www.law.com/corpcounsel/2018/11/09/gdpr-fine-against-portuguese-hospital-puts-health-care-providers-on-alert/; Irwin, Luke. "Portuguese hospital appeals GDPR fine." IT Governance blog. November 15, 2018. https://www.itgovernance.eu/blog/en/portuguese-hospital-appeals-gdpr-fine

32 Rosemain, Mathieu. "France fines Google $57 million for European privacy rule breach. Reuters Business News. January 21, 2019. https://www.reuters.com/article/us-google-privacy-france/france-fines-google-57-million-for-european-privacy-rule-breach-idUSKCN1PF208

33 "Online platforms: Commission sets new standards on transparency and fairness." European Commission. April 26, 2018. http://europa.eu/rapid/press-release_IP-18-3372_en.htm; Cowdrey, Katherine. "EC considers new law to tackle unfair online trading practices." *The Bookseller*. May 10, 2017. https://www.thebookseller.com/news/european-commission-pledges-further-action-tackle-online-platforms-unfair-contracts-549606

34 Anupam, Suprita. "Will EU's New Copyright Directive Benefit Content Creators Or Stifle Freedom Of Digital Expression?" Inc 42. September 19, 2018. https://inc42.com/features/will-eus-new-copyright-directive-benefit-content-creators-or-stifle-freedom-of-digital-expression/

35 Martin, Timothy W. and Sam Schechner. "Facebook, Google May Face Billions in New Taxes Across Asia, Latin America." *The Wall Street Journal*. October 28, 2018. https://www.wsj.com/articles/countries-push-digital-taxes-on-tech-giants-1540742400; Ahmed, Kamal. "EU pushes for new tax on tech giants 'by Christmas.'" BBC News. October 10, 2018. https://www.bbc.com/news/business-45813754

36 Field, Matthew. "France goes it alone to levy digital tax on tech giants from January 1." The Telegraph. December 17, 2018. https://www.telegraph.co.uk/technology/2018/12/17/france-goes-alone-levy-digital-tax-tech-giants-january-1/; Dobush, Grace. "The EU Can't Agree on a Digital Tax — but Silicon Valley's Still Going to Pay." Fortune. January 3, 2019. http://fortune.com/2019/01/03/eu-digital-tax-silicon-valley/

37 Minter, Adam. "Why Big Brother Doesn't Bother Most Chinese." Bloomberg. January 24, 2019. https://www.bloomberg.com/opinion/articles/2019-01-24/why-china-s-social-credit-systems-are-surprisingly-popular

38 Zhao, Leo and Lulu Xia. "China's Cybersecurity Law: An Introduction for Foreign Businesspeople." *China Briefing*. March 1, 2018. https://www.china-briefing.com/news/chinas-cybersecurity-law-an-introduction-for-foreign-businesspeople/; Wagner, Jack. "China's Cybersecurity Law: What You Need to Know." *The Diplomat*. June 1, 2017. https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

39 Ramey, Melanie. "Brazil's New General Data Privacy Law Follows GDPR Provisions." *Inside Privacy*. August 20, 2018. https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/; Merwin, Radhika. "All you wanted to know about Personal Data Protection Bill 2018." *Hindu Business Line*. August 6, 2018. https://www.thehindubusinessline.com/opinion/columns/slate/all-you-wanted-to-know-about/article24617362.ece; Nishi, Michihiro. "Data Protection in Japan to Align With GDPR." Skadden.com. September 24, 2018. https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr

40 Draft Ethics guidelines for trustworthy AI." European Commission. December 18, 2018. https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai; Guerrini, Federico. "AI With An Ethic: European Experts Release Draft Guidelines." *Forbes*. December 23, 2018. https://www.forbes.com/sites/federicoguerrini/2018/12/23/from-mass-surveillance-to-killer-robots-eu-experts-want-your-feedback-to-create-trustworthy-ai/#48e3bc777ddf

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
February 2019

88023088USEN-01